UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/870,610	05/31/2001	Dwip N. Banerjee	AUS9-2001-0361-US1	1787

40412 7590 01/09/2008

IBM CORPORATION- AUSTIN (JVL)
C/O VAN LEEUWEN & VAN LEEUWEN
PO BOX 90609
AUSTIN, TX 78709-0609

EXAMINER	
BAYARD, DJENANE M	

ART UNIT	PAPER NUMBER
2141	

MAIL DATE	DELIVERY MODE
01/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte DWIP N. BANERJEE, VINIT JAIN,
and VASU VALLABHANENI

Appeal 2007-2431
Application 09/870,610[1]
Technology Center 2100

Decided: January 9, 2008

Before JOSEPH F. RUGGIERO, MAHSHID D. SAADAT,
and JEAN R. HOMERE, *Administrative Patent Judges*.

HOMERE, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134 from the Examiner's Final Rejection of claims 1, 5, 8, 11, 14, 18, and 21 through 30. Claims 2 through 4, 6, 7, 9, 10, 12, 13, 15 through 17, 19, and 20 have been canceled. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

---

[1] Filed on May 31, 2001. The Real Party in interest in this appeal is International Business Machines.

The Invention

Appellants invented a method and system for preventing a client's malicious attacks at a server by monitoring the client's requests to the server. Particularly, the invention blocks the client's access to the server if the client's request exceeds a stored socket limit or stored packet limit within a given time interval. (Spec. 5.)

An understanding of the invention can be derived from exemplary independent claims 1 and 27, which read as follows:

1. A method for preventing malicious network attacks said method comprising:

providing a test script, the test script including one or more attack simulations;

processing the attack simulations included in the test script;
determining whether to change one or more configuration settings based upon the processing;

changing one or more of the configuration settings based upon the determination;

receiving a packet from a client computer;

identifying the client computer by a source IP address;

calculating a number of packets received using the source IP address during a time interval, wherein the calculating includes:

retrieving a number of packets received that correspond to the source IP address;

and

incrementing the number of packets received;

comparing the incremented number of packets received with one or more of the configuration settings;

determining an action from a plurality of actions based on the comparing; and

executing the action.

27. A method for preventing malicious network attacks on a server computer from a client computer that accesses the server computer via a computer network, said method comprising:

executing a test script that includes one or more attack simulations from the client computer, the execution of the test script including:

receiving, at the server computer, one or more packets from the client computer and one or more open socket requests form the client computer;

deciding a packet threshold for the client computer, the deciding including:

determining a number of packets received from the client computer during a time interval;

incrementing the number of packets received from the client computer; and
comparing the number of packets received with a packet limit stored at the server computer;

computing an open socket threshold for the client computer, the computing including:

determining a number of opened sockets for the client computer;

incrementing the number of opened sockets for the client computer;

comparing the number of sockets opened from the client computer to a socket limit stored at the server computer; and

evaluating the packet limit and the socket limit used during the attack simulations, the evaluating including:

analyzing the performance of the server computer during the simulation; and

adjusting a server configuration setting based on the analysis, wherein the

adjusted server configuration setting is selected from group consisting of the stored packet limit and the stored socket limit.

The Examiner relies upon the following prior art to reject the claims on appeal:

Lockhart	US 6,189,035 B1	Feb. 13, 2001
Porras	US 6,321,338 B1	Nov. 20, 2001
Carlson	US 6,381,649 B1	Apr. 30, 2002
Barrett	US 2002/0059454 A1	May 16, 2002
Goldstone	US 2002/0101819 A1	Aug. 01, 2002
Lewis	US 2003/0110396 A1	Jun. 12, 2003
Ptacek	US 6,636,972 B1	Oct. 21, 2003

The Examiner rejects the claims on appeal as follows:

A. Claims 1, 8, 14, and 28 through 30[2] stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lewis and Lockhart.

[2] We note that the Examiner's statement of the rejection omits claims 28 through 30. (Ans. 30.)

B. Claims 5, 11, and 18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lewis, Lockhart, and Goldstone.
C . Claims 21, 23, and 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lewis, Lockhart, and Carlson.
D. Claims 22, 24, and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lewis, Lockhart, and Porras.
E. Claim 27 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Ptacek, Lockhart, and Barrett.

First, Appellants contend that the combination of Lewis and Lockhart does not render claims 1, 5, 8, 11, 14, 18, and 28 through 30 unpatentable since the combination of the cited references does not result in a reasonable expectation of success. Particularly, Appellants assert the following:

> [t]he Examiner fails to consider all words in Appellants' claims as a whole during the Examiner's patentability judgment. Appellants clearly claim "**configuration settings**" in Appellants' third element, and the "**configuration settings**" in Appellants' fourth element. Hence, Appellants are claiming the **same** configuration settings in each of these elements. Appellants assert, however, that the Examiner does not view Appellants' "configuration settings" on a consistent basis for each element, and therefore the Examiner does not view Appellants' claim 1 as a whole.

(App. Br. 11.)

Further, Appellants assert the following:

> As can be seen, Lockhart's "*predetermined threshold*" is in no way analogous to Lewis's "*identified events*" and, therefore, they may not be interchanged. Since the Examiner does, in fact, interchange these two items, the Examiner does not view Appellants' invention as

> a whole, but rather dissects Appellants' independent claims into discrete elements and evaluates the elements in isolation.

(Reply Br. 2.)

Appellants reiterate these same arguments to distinguish claims 21 through 26 over the prior art of record as set forth above. In response, the Examiner submits that one of ordinary skill in the art would have combined Lewis' "identified temporal attack precursors and triggers" with Lockhart's "predetermined threshold number of received packets" to arrive to the claimed configuration settings. (Ans. 12-14.)

Next, Appellants contend that the combination of Ptacek, Lockhart, and Barrett does not render claim 27 unpatentable. Particularly, Appellants contend that the cited combination does not teach adjusting a server configuration based a performance analysis of the server wherein the configuration setting is selected from a stored packet limit and a stored socket limit. (App. Br. 15, Reply Br. 4.) In response, the Examiner submits that Ptacek's disclosure of a simulation software that detects whether computer hosts are vulnerable to certain attacks, taken in combination with Lockhart's disclosure of a predetermined threshold number of received packets and Barrett's disclosure of a predetermined threshold number of open sockets teach the claimed invention. (Ans. 14-15.)

ISSUES

The *pivotal* issues in the appeal before us are as follows:

A. Have Appellants shown[3] that the Examiner failed to establish that the combined disclosures of Lewis and Lockhart render the claimed invention unpatentable under 35 U.S.C. § 103(a)? Particularly, does Lewis' disclosure of identified temporal attack precursors and triggers, taken in combination with Lockhart's disclosure of a predetermined threshold number of received packets teach the claimed configuration settings?

B. Have Appellants shown that the Examiner failed to establish that the combined disclosures of Ptacek, Lockhart, and Barrett render the claimed invention unpatentable under 35 U.S.C. § 103(a)? Particularly, does Ptacek's disclosure of a simulation software that tests computer hosts for certain threats, taken in combination with Lockhart's disclosure of a predetermined threshold number of received packets, and Barrett's

[3] In the examination of a patent application, the Examiner bears the initial burden of showing a prima facie case of unpatentability. *In re Piasecki,* 745 F.2d 1468, 1472 (Fed. Cir. 1984). When that burden is met, the burden then shifts to the applicant to rebut. *Id.*; *see also In re Harris*, 409 F.3d 1339, 1343-44 (Fed. Cir. 2005) (finding rebuttal evidence unpersuasive). If the applicant produces rebuttal evidence of adequate weight, the prima facie case of unpatentability is dissipated. *Piasecki*, 745 F.2d at 1472. Thereafter, patentability is determined in view of the entire record. *Id.* However, Appellant has the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)).

disclosure of a predetermined threshold number of open sockets teach the claimed invention?

FINDINGS OF FACT

The following findings of fact are supported by a preponderance of the evidence.

The Invention

1. Appellants' invention uses an attack blocking logic (130) that monitors packet and socket requests (140) issued by client computers (165, 180) to prevent malicious attacks at a hosting server (100). (Spec. 8-9.) A system admin configuration (230) includes a "packets allowed" unit (235) and a time interval unit (240) that contains the number of packets allowed for each client within a specified time interval. The system administrator also includes a server port unit (245) that contains how many allowable sockets each client may have. Upon determining that the client's request has exceeded the allotted number of packets or open sockets, the system administrator (230) informs an IP packet daemon (210) to block the client's access. The system administrator (230) may subsequently increase or decrease the security level by adjusting factors such as time interval, the number of packets or open sockets allowed. (*Id.* 10-11.)

2. As depicted in Figure 3, upon loading a configuration file (310) on a server, a test script including a plurality of attack simulations is run to determine whether to change the configuration settings of the server. If the simulation results indicate that the server is vulnerable to certain attacks, the configuration settings are then adjusted accordingly. (*Id.* 11-12.)

3. Upon receiving a plurality of packets and/or open sockets from the client computer, the system administrator identifies the IP source address of

the client to determine the number of packets received from said client during a particular time interval, as well as the number of open sockets received from the client. The system administrator subsequently compares the received number of packets and/or open sockets with the predetermined number of packets and/or open sockets to determine if the client request has exceeded its preset limits. If so, the client is blocked from accessing the server. (*Id.*)

The Prior Art Relied Upon

4. Lewis discloses a system for preventing attacks in a communication network. As shown in Figure 1, Lewis discloses that during the simulation of a network attack, data is collected from the network. The collected data is analyzed to identify specific precursors of the attack. Responsive triggers to the identified precursors are then placed in the network to monitor the presence of such precursors in a client request. Upon finding a matching precursor in a client request, the client is blocked from accessing the network. (Page 4, par. 0051-0052.)

5. Lewis further discloses that the data is collected in any manner known in the art. The collected data can be from variety of known media, including traffic media.[4] (Page 4, par. 0047.) The precursors identified from analyzing

[4] Particularly, Lewis states that:

> [T] he second phase is the actual DDoS attack. Under command from the Master, the Slaves generate network traffic to bring down the Target system. Any system connected to the Network can be a Target. Routers and web servers are typical examples. *Although the nature of the traffic (UDP, ICMP, etc.) differs among the various types of DDoS attacks, the common factor is the abnormally large number of connections attempted to the Target system during a very small interval of time. Although the processing of this traffic usually shuts down the Target system, it typically does not matter how the Target handles the packets; the volume of traffic is so great that the whole*

the collected data include any and all variables that manifest aberrant values or activity levels just prior to the onset of the attack. (Page 4, par. 0048.)

6. Lockhart discloses a method for protecting a network from packet overload by limiting the number of data packets that pass through the internal network without degrading its operation. As depicted in Figure 2, Lockhart discloses a data packet gate (20) that maintains a recent packet count for each IP source that sends packets to the internal network. Upon receiving a packet, the data packet gate identifies the IP source of the incoming packet. If the total count of packets received for the identified IP source exceeds a predetermined threshold number of packets, then the IP source is denied access. (Col. 2, ll. 40-54; col. 3, ll. 25-27, col. 3, l. 65- col. 4, l. 20.)

7. Ptacek discloses an executable script for performing a network audit by simulating an exchange of network protocol compliant packets. Particularly, Ptacek uses a custom attack simulation language (CASL) that simulates attacks against a host to see if the host is vulnerable to certain identified attacks. An example of such attacks includes attempting to connect to a port in the network without actually opening a connection. (Col. 6, ll. 29-57.)

8. Barrett discloses a system that enables an online service provider to identify an e-mail sender before routing the e-mail to a designated recipient. Particularly, upon receiving an email, the system determines the number of connections that are open with the sender. If the number of open

---

network becomes congested with artificial traffic. The congestion does not allow legitimate traffic to pass, thus rendering the Target inaccessible and making the DDoS attack ultimately successful. (Page 5, par. 0062, emphasis added.)

connections exceeds a predetermined threshold number, the e-mail is blocked. (Page 1, par. 0006.)

OBVIOUSNESS

"Section 103 forbids issuance of a patent when 'the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.'" *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1734 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) where in evidence, so-called secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966). *See also KSR*, 127 S. Ct. at 1734 ("While the sequence of these questions might be reordered in any particular case, the [*Graham*] factors continue to define the inquiry that controls.")

"The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results."). *Leapfrog Enter., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1161 (Fed. Cir. 2007) (quoting *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740-41(2007)).)). "One of the ways in which a patent's subject matter can be proved obvious is by noting that there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims." *KSR*, 127 S. Ct. at 174.

Discussing the obviousness of claimed combinations of elements of prior art, *KSR* explains:

> When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, §103 likely bars its patentability. For the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill. *Sakraida* [*v. AG Pro, Inc.,* 425 U.S. 273 (1976)] and *Anderson's-Black Rock*[*, Inc. v. Pavement Salvage Co*., 396 U.S. 57 (1969)] are illustrative—a court must ask whether the improvement is more than the predictable use of prior art elements according to their established functions.

KSR, 127 S. Ct. at 1740 at 1396. Where the claimed subject matter cannot be fairly characterized as involving the simple substitution of one known element for another or the mere application of a known technique to a piece of prior art ready for the improvement, a holding of obviousness can be based on a showing that there was "an apparent reason to combine the known elements in the fashion claimed." *KSR*, 127 S. Ct. at 1740-41, at 1396. Such a showing requires "some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *Id.*, 127 S. Ct. at 1741, 82 USPQ2d at 1396 (quoting *In re Kahn*, 441 F.3d 977, 987(Fed. Cir. 2006)).

The reasoning given as support for the conclusion of obviousness can be based on interrelated teachings of multiple patents, the effects of demands known to the design community or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art. *KSR*, 127 S. Ct. at 1740-41at 1396. *See also Dystar*, 464 F.3d at 1368

("[A]n implicit motivation to combine exists not only when a suggestion may be gleaned from the prior art as a whole, but when the "improvement" is technology-independent and the combination of references results in a product or process that is more desirable, for example because it is stronger, cheaper, cleaner, faster, lighter, smaller, more durable, or more efficient. Because the desire to enhance commercial opportunities by improving a product or process is universal—and even common-sensical—we have held that there exists in these situations a motivation to combine prior art references even absent any hint of suggestion in the references themselves. In such situations, the proper question is whether the ordinary artisan possesses knowledge and skills rendering him capable of combining the prior art references."); *Leapfrog*, 485 F.3d at 1162 at 1691 (holding it "obvious to combine the Bevan device with the SSR to update it using modern electronic components in order to gain the commonly understood benefits of such adaptation, such as decreased size, increased reliability, simplified operation, and reduced cost").

Also, a reference may suggest a solution to a problem it was not designed to solve and thus does not discuss. *KSR*, 137 S. Ct. at 1742 at 1397 ("Common sense teaches . . . that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle. . . . A person of ordinary skill is also a person of ordinary creativity, not an automaton.").

The prior art relied on to prove obviousness must be analogous art. As explained in *Kahn*,

> the "analogous-art" test . . . has long been part of the primary Graham analysis articulated by the Supreme Court. *See Dann* [*v. Johnston*,] 425 U.S. [219,] 227-29 (1976), *Graham*, 383 U.S. at 35. The analogous-art test requires that the Board show that a reference is either in the field of the applicant's endeavor or is reasonably pertinent to the problem with which the inventor was concerned in order to rely on that reference as a basis for rejection. *In re Oetiker*, at 1447. References are selected as being reasonably pertinent to the problem based on the judgment of a person having ordinary skill in the art. *Id.* ("[I]t is necessary to consider 'the reality of the circumstances,'—in other words, common sense—in deciding in which fields a person of ordinary skill would reasonably be expected to look for a solution to the problem facing the inventor." (quoting *In re Wood*, 599 F.2d 1032 (C.C.P.A. 1979))).

Kahn, 441 F.3d at 986-87, at 1335-36. *See also In re Clay*, 966 F.2d 656, 659 (Fed. Cir. 1992) ("[a] reference is reasonably pertinent if, even though it may be in a different field from that of the inventor's endeavor, it is one which, because of the matter with which it deals, logically would have commended itself to an inventor's attention in considering his problem.").

In view of KSR's holding that "*any* need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed," 127 S. Ct. at 1742, at 1397 (emphasis added), it is clear that the second part of the analogous-art test as stated in *Clay*, *supra*, must be expanded to require a determination of whether the reference, even though it may be in a different field from that of the inventor's endeavor, is one which, because of the matter with which it deals, logically would have commended itself to an artisan's (not necessarily the inventor's) attention in considering *any* need or problem known in the field of endeavor. Furthermore, although under *KSR*

it is not always necessary to identify a known need or problem as a motivation for modifying or combining the prior art, it is nevertheless always necessary that the prior art relied on to prove obviousness be analogous. *See KSR*, 127 S. Ct. at 1739, at 1395 ("The Court [in *United States v. Adams,* 383 U.S. 39, 40 (1966)] recognized that when a patent claims a structure already known in the prior art that is altered by the mere substitution of one element for another *known in the field*, the combination must do more than yield a predictable result.") (emphasis added). *See also Sakraida*, 425 U.S. at 280 ("Our independent examination of that evidence persuades us of its sufficiency to support the District Court's finding 'as a fact that each and all of the component parts of this patent . . . were old and well-known throughout the dairy industry long prior to the date of the filing of the application for the Gribble patent.'").

ANALYSIS

Claims 1, 5, 8, 11, 14, 18, 21 through 26, and 28 through 30

Independent claim 1 recites comparing an incremented number of packets received from an identified client computer with one or more configuration settings. (App. Br. 17, Claim Appendix.) We agree with the Examiner that the combined disclosures of Lewis and Lockhart reasonably teach this limitation.

As detailed in the Findings of Fact (FF) section above, Appellants' claimed "configuration settings" (that are compared with the incremented packets for a particular client) refer to a stored packet limit allowed for each client within a specified time interval. (FF 1 and 3.) Similarly, Lewis

discloses comparing precursors identified in a simulated attack with precursors (events) in an incoming request from a client computer. (FF 4.) Upon finding a match between these precursors, the client is blocked from accessing the network. (*Id.*) Lewis further discloses that the stored precursors being compared include events indicating traffic congestion on the network. (FF 5.) Additionally, Lockhart discloses comparing an incremented number of data packets of an identified IP source for a client computer with a predetermined threshold number. (FF 6.) If the incremented number of packets exceeds the predetermined threshold number, the client request is blocked. (*Id.*) Lockhart discloses limiting for each client the number of packets that pass through the internal network as a precondition for avoiding packet overload (i.e. network congestion). (*Id.*) It is therefore our view that one of ordinary skill would have readily recognized that Lewis' apparatus, taken in combination with Lockhart's disclosure, would have *predictably* resulted in a system that compares an incremented number of packets received from an identified client computer with a configuration setting indicating a stored packet limit.[5] The ordinarily skilled artisan would have thus recognized that Lockhart's disclosure of limiting the number of packets that pass through the network for each client resolves, inter alia, the traffic congestion problem that Lewis sought to prevent by using pre-identified precursors. Hence, the ordinarily skilled

[5] The Supreme Court has held that in analyzing the obviousness of combining elements, a court need not find specific teachings, but rather may consider "the background knowledge possessed by a person having ordinary skill in the art" and "the inferences and creative steps that a person of ordinary skill in the art would employ." *See KSR*, 127 S. Ct. at 1740-41. To be nonobvious, an improvement must be "more than the predictable use of prior art elements according to their established functions." *Id.* at 1740.

artisan would have readily appreciated that the Lewis-Lockhart combination teaches utilizing a precursor or configuration setting, particularly identified as a stored packet limit to reduce traffic congestion by preventing malicious attacks thereon. It follows that the Examiner did not err in rejecting independent claim 1as being unpatentable over the combination of Lewis and Lockhart.

Appellants did not provide separate arguments with respect to the rejection of claims 1, 5, 8, 11, 14, 18, 21 through 26, and 28 through 30. Appellants merely repeat the same argument made for claim 1 for claims 5, 8, 11, 14, 18, 21 through 26, and 28 through 30. (App. Br. 9-13). Therefore, we select independent claim 1 as being representative of the cited claims. These claims consequently fall together with representative claim 1. *See also* 37 C.F.R. § 41.37(c)(1)(vii).

Claim 27

Claim 27 requires adjusting a server configuration based on performance analysis of the server wherein the configuration setting is selected from a stored packet limit and a stored socket limit. (App. Br. 22, claims Appendix.) We agree with the Examiner that the combined disclosures of Ptacek, Lorkhart, and Barrett reasonably teach that limitation.

Ptacek discloses a CASL that simulates attacks against a host to see if the host is vulnerable to certain identified attacks such as attempting to connect to a port without actually opening a connection. (FF 7.) As indicated in our discussion above, Lockhart discloses using a stored packet limit to prevent traffic congestion on the network. (FF 6.) Additionally, Barrett discloses a service provider that blocks an incoming e-mail upon

determining that the number of open sockets from the e-mail sender exceeds a predetermined threshold number. (FF 8.)

It is our view that one of ordinary skill in the art would have readily recognized that the combination of Ptacek, Lockhart and Barrett teaches auditing a network through simulated attacks by attempting to exceed a stored packet limit and a stored socket limit. The ordinarily skilled artisan would have appreciated that after performing the audit, if it is discovered that the client exceeds the stored packet limit or the stored socket limit, the network would necessarily be adjusted to correct such noted deficiencies. Common sense would have guided the ordinarily skilled artisan to use simulation results to adjust the configuration settings of the server. Therefore, on the record before us, we conclude that the proffered combination would suggest to the skilled artisan to utilize the result of the simulation to adjust the server configuration settings consisting of the stored packet limit and the stored socket limits. It follows that the Examiner did not err in rejecting independent claim 27 as being unpatentable over the combination of Ptacek, Lockhart, and Barrett.

1Rejection under 37 CFR § 41.50(b)

We make the following new ground of rejection using our authority under 37 CFR § 41.50(b). Claim 27 is rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lewis, Lockhart, and Barrett. As detailed in our discussion of claim 1 above, the combination of Lewis and Lockhart teach simulating a server with attacks to identify precursors including a stored packet limit, which is used to subsequently adjust the configuration settings of the server. (FF 4-6.) Further, as indicated above,

Barrett teaches using a stored socket limit as a precursor to reduce congestion. (FF 8.) Therefore, one of ordinary skill would have readily recognized that the combination of Lewis, Lockhart, and Barrett would have *predictably resulted* in a simulation of the server to identify precursors including a stored packet limit and a stored socket limit to subsequently adjust the configuration settings of the server.

CONCLUSIONS OF LAW

On the record before us, we conclude that:

A. Appellants have not shown that the Examiner failed to establish that the combination of Lewis and Lockhart renders claims 1, 8, 14, and 28 through 30 unpatentable under 35 U.S.C. § 103(a).

B. Appellants have not shown that the Examiner failed to establish that the combination of Lewis, Lockhart, and Goldstone renders claims 5, 11, and 18 unpatentable under 35 U.S.C. § 103(a).

C . Appellants have not shown that the Examiner failed to establish that the combination of Lewis, Lockhart, and Carlson renders claims 21, 23, and 25 unpatentable under 35 U.S.C. § 103(a).

D. Appellants have not shown that the Examiner failed to establish that the combination of Lewis, Lockhart, and Porras renders claims 22, 24, and 26 unpatentable under 35 U.S.C. § 103(a).

E. Appellants have not shown that the Examiner failed to establish that the combination of Ptacek, Lockhart, and Barrett renders claim 27 unpatentable under 35 U.S.C. § 103(a).

F. The combination of Lewis, Lockhart, and Barrett renders claim 27 unpatentable under 35 U.S.C. § 103(a).

DECISION

A. We affirm the Examiner's decision rejecting claims 1, 5, 8, 11, 14, 18, and 21 through 30.

B. We enter a new ground of rejection rejecting claim 27.

This decision contains a new ground of rejection pursuant to 37 CFR § 41.50(b) (effective September 13, 2004, 69 Fed. Reg. 49960 (August 12, 2004), 1286 Off. Gaz. Pat. Office 21 (September 7, 2004)). 37 CFR § 41.50(b) provides "[a] new ground of rejection pursuant to this paragraph shall not be considered final for judicial review."

37 CFR § 41.50(b) also provides that the appellant, WITHIN TWO MONTHS FROM THE DATE OF THE DECISION, must exercise one of the following two options with respect to the new ground of rejection to avoid termination of the appeal as to the rejected claims:

> (1) *Reopen prosecution*. Submit an appropriate amendment of the claims so rejected or new evidence relating to the claims so rejected, or both, and have the matter reconsidered by the examiner, in which event the proceeding will be remanded to the examiner. . . .
>
> (2) *Request rehearing*. Request that the proceeding be reheard under § 41.52 by the Board upon the same record. . . .

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

pgc

IBM CORPORATION- AUSTIN (JVL)
C/O VAN LEEUWEN & VAN LEEUWEN
PO BOX 90609
AUSTIN TX 78709-0609